(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/059849 A1

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/TR01/00003

(22) International Filing Date: 26 January 2001 (26.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants and
(72) Inventors: **PAK, Ihsan, Iskender** [TR/TR]; Konutkent II A4 Blok D.32, 06530 Ankara (TR). **ÖZSOY, Mete** [TR/TR]; Mahatma Gandhi Cad. 21/10, G.O.P., 06700 Ankara (TR).

(74) Agent: **ANKARA PATENT BUREAU LTD.**; Sehit Adem Yavuz Sokak 8/22, Kizilay, 06440 Ankara (TR).

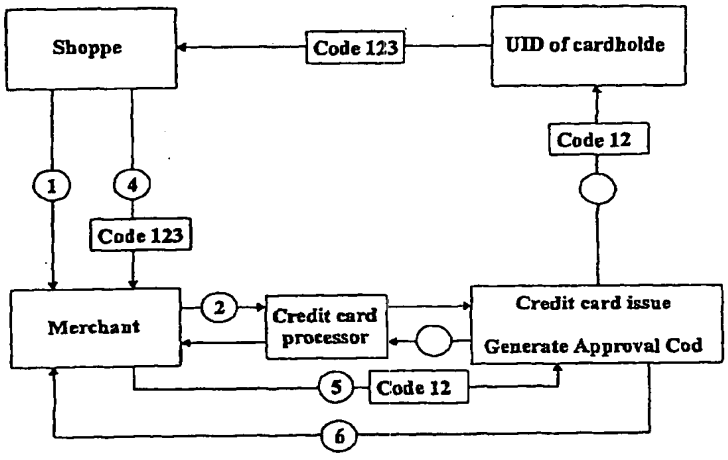
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR PREVENTING CREDIT CARD FRAUD



(57) Abstract: The present invention provides a method and system for the prevention of credit card fraud utilizing a communication network. A credit cardholder, a Unique Identification Device (UID), a merchant, a credit card issuer and the generation of an approval code constitute the main components of the method and system. The method and system can be applied to both traditional credit card transactions and "card not present" credit card transactions. The invention does not require changes to be made to current authorization systems. It compliments current systems by providing a private channel of communication between the credit card issuer and the cardholder that is independent of the usual channel used to conduct a transaction.

WO 02/059849 A1

METHOD AND SYSTEM FOR PREVENTING CREDIT CARD FRAUD

The present invention relates to a method and system for the prevention of credit card fraud through the use of a communication network.

Credit Cards and their use as payment instruments for the purchase of goods and services are widely accepted. They are used globally through an established infrastructure, which efficiently and conveniently allows payments to be made in most areas of the world. A credit card is usually issued to an individual or a company by a financial institution or by a credible merchant with established ties to a bank. A credit card holder may present it as a payment to a merchant; the card bearer must reimburse the credit card company the amount of the sale later.

The most popular method of payment in e-commerce is the credit card. The purchaser browses the virtual stores or merchants and selects the items of interest by placing them in a shopping cart. When a decision is made to purchase the items selected, the customer is directed to the checkout. During the checkout phase, customer is requested to enter credit card data and other personal information. Upon completion of these steps, the merchant's virtual store processes the data and sends it to a credit card processor, and waits for authorization; similar to traditional card swipe (POS) methods. Once the credit card processor has given the authorization, the merchant accepts the order and delivers the ordered item to the purchaser. At this stage, the amount of the purchase made awaits to be deducted from the credit card holder's account. These types of credit card transactions are very similar in nature to mail order/phone order (MOTO) transactions. These transactions along with E-commerce transactions are categorized by credit card companies as "card not present" transactions. They are regarded as more risky. The rates charged by the merchant account providers for credit card transactions in which the actual credit card is not present are generally higher than card swipe rates charged in physical "card present" transactions. This is due to the higher chance of fraud or nonpayment in the "card not present" transactions.

Unfortunately, merchants and the credit card companies alike are suffering from the credit card fraud. Merchants are responsible for chargebacks and credit card companies face the risk of a reduction in the number of merchants who are willing to accept this type of transaction. In addition, many consumers are reluctant to shop online, fearing fraudulent use of their credit card. The rate of this sort of crime is increasing and is now at an alarming level. It is seen as a major obstacle to the growth of e-commerce.

Most of the credit card information used for the fraudulent online purchases apparently is obtained in the old-fashioned way: stolen from mailboxes or "swiped" through a card reader by accomplices working in restaurants or stores. This stolen credit card information is then transmitted to the thief or thieves overseas, who begin their electronic assault on Internet merchants by charging as much merchandise as they can in as short a time as possible. In some cases, they will attempt to ship the goods directly to the country they are operating out of, where the credit card address-verification system can't be used because of stringent privacy laws. In other cases, since many Internet sellers are now wary of shipping expensive merchandise overseas, they will enlist accomplices in the Merchant's home country who set up "drop sites" in vacant homes or rent living quarters under false names. By the time the e-merchant realizes the purchase was made using stolen credit cards, the goods and the thieves are gone. These days, a credit card number is a valuable commodity to thieves. Thieves do not need the physical credit card to use somebody's credit card number, particularly in this era of Internet and catalog shopping; the same applies to debit cards. A thief armed with a debit card number can go on a shopping spree, financed by the cardholder's checking account. Tech-savvy criminals are devising new ways to get their hands on card information. They've figured out that card fraud beats holding up someone at gunpoint. Instead, they're hacking into Internet databases filled with customer card data and copying account details encoded on a card's magnetic stripe. It appears as if credit card fraud is the bank robbery of the future.

Current solutions vary; Currently, none of the solutions completely eliminate fraud. But designing Web sites that require several pieces of information about the card and the potential buyer helps a lot. Those items can then be run through screening software that looks for anomalies and red flags, generating a fraud risk score. Most of the current approaches focus on huge customer databases that track and monitor customer activity to understand behavior patterns of shoppers. Based on the collected data and its processing they aim to screen out shopping activity which does not match past behavior.

Combating fraud has always been a cost of doing business, long before e-commerce came along. But another element unique to Internet merchants is the cost of losing valuable business as a result of fraud protection efforts. Antifraud systems use algorithms to detect risk, and the systems will reject an order if it falls within a designated realm.

Small merchants can afford to phone each customer whose order is deemed too risky. But retailers that deploy such systems on a large scale are forced to let orders fall by the wayside, meaning they could be losing valuable customers. Some merchants are declining large percentage of their orders to minimize fraud, which amounts to significant amount of business.

The Credit Card companies have been active in implementing methods to prevent credit card fraud. One of these methods is the CVV2/CVC2; a three-digit security code that is printed on the back of cards. The number appears in reverse italic

at the top of the signature panel at the end (see sample). This program helps validate that a genuine card is being used during a transaction. All MasterCard cards, both credit and debit, were required to contain CVC2 by January 1, 1997; all Visa cards must contain CVV2 by January 1, 2001. Card-not-present merchants are being directed to ask cardholders for CVV2/CVC2 when cardholders place orders. Merchants ask the cardholder to read this code from the card. The merchant then asks for CVV2/CVC2 verification during the authorization process. The issuer (or processor) validates the CVV2/CVC2 and relays the decline/approve results during the authorization process. Merchants, by using the CVV2/CVC2 results along with the Address Verification Service (AVS) and authorization responses, can then make more informed decisions about whether to accept transactions. In addition, merchants using CVV2/CVC2 can expect to reduce their chargebacks by as much as 26 percent. Previously the three-digit CVV2 or CVC2 number followed the 16-digit account number printed on the card's signature panel. The 16-digit account number is now truncated to four digits on the signature panel. Beginning March 31, 2000, cards issued by Equifax will show the last four digits of the account number followed by the three-digit CVV2 or CVC2 number on the card signature panel. This change makes it easier for cardholders to sign their cards. It also makes it easier for merchants to compare the signature on the card to the one on the sales draft; no longer will those 19 digits (16 + 3) get in the way of verifying a signature!

The object of the present invention is to provide a method and system for the prevention of credit card fraud through the use of a communication network.

Figure 1.a. is a general working diagram of single code generation implementation in a legitimate transaction.

Figure 1.b. is a general working diagram of single code generation implementation in an attempted fraudulent use

Figure 1.c. is system flowchart of single code generation implementation.

Figure 2.a. is a general working diagram of shopper check-code generation implementation in a legitimate transaction.

Figure 2.b. is a general working diagram of shopper check-code generation implementation in an attempted fraudulent use

Figure 2.c. is system flowchart of shopper check-code generation implementation.

Figure 3.a. is a general working diagram of merchant check-code generation implementation in a legitimate transaction.

Figure 3.b. is a general working diagram of merchant check-code generation implementation in an attempted fraudulent use

Figure 3.c. is system flowchart of merchant check-code generation implementation.

Figure 4. is a diagram of information requested by the merchant to process and validate the credit card.

Figure 5. is a diagram that illustrates the method by which approval codes are generated.
Figure 6 is a diagram of a look up server.

The present invention provides a method and system for the prevention of credit card fraud utilizing a communication network. A credit cardholder (shopper), a Unique Identification Device (UID), a merchant, a credit card issuer and the generation of an approval code constitute the main components of the method and system.

The method and system can be applied to both traditional credit card transactions ("card present-POS) and "card not present" credit card transactions (VPOS- i.e. internet purchases, MOTO – i.e.: mail or telephone orders). The invention does not require changes to be made to current authorization systems. It compliments current systems by providing a private channel of communication between the credit card issuer and the cardholder that is independent of the usual channel used to conduct a transaction.

For the purposes of this description we will outline 4 stages in the completion of a transaction using a credit or debit card.

Validation; information necessary for the processing of the credit card is checked to be valid. i.e. of the correct type and length. Credit card numbers may only be valid if they are 16 digits long.

Authorization; when a credit card issuer receives a request to process a credit card certain checks are made. The credit card number must match an existing account. The account must be active and sufficient funds must be available. This process will be referred to as authorization. When a transaction is authorized funds are allocated for transfer to the merchant's account.

Verification; the invention offers the ability to verify the identity of a shopper attempting to use a credit card to make a purchase. The invention can determine whether or not the shopper is the cardholder for a specific account. This process is referred to as verification.

Approval; when a transaction has been validated, authorized, and verified it is referred to as an approved transaction.

The cardholder is an individual or a company, having an active credit card account with which transactions can be processed. Also used to refer to the actual owner of an identification device supplied by any organization used for verifying the relationship between the organization and the individual.

The shopper is any individual, company, government organization or private organization that initiates an action which requires approval of a purchasing process using credit card. The shopper may or may not be the actual cardholder

himself/herself. If the shopper is not the cardholder, he/she is attempting to use the credit card fraudulently.

The credit card issuer is a public or private organization that issues credit cards or debit cards to be used for the purchase of merchandise or services. Credit card issuer then bills the customer and is responsible for maintaining the cardholder's personal and card related data. The term may also be used to refer to an agency acting on behalf of the issuing body.

Unique Identification Device (UID) refers to a device, specific to the cardholder, that provides communication or sharing of information between parties. Such a device has a privacy property that is known to the device owner. Examples of UID's include GSM phones, e-mail accounts, pagers, personal computers, Internet enabled PDA's (Personal Digital Assistants) and similar devices. UID's may have the capacity to store and execute programs. A UID may be capable of only unidirectional communication. A pager is an example of such a UID. It can receive a message but cannot respond to it. Other UID's allow for interactive bi-directional communication. A telephone (wireline) or mobile phone (wireless) may receive and send voice and text messages such as those used in SMS (Short Message Service). An email account may send and receive messages.

An approval code is generated and exchanged between the credit card issuer, the shopper (cardholder), and/or the merchant for identification, verification and purchase approval. An approval code is a series of alphanumeric characters and is only accessible by the credit card issuer, the cardholder and cardholder-authorized third parties via the cardholder's UID. By exchanging the approval code among the involved parties, the invention verifies the identity of the cardholder and prevents unauthorized use.

The method and system and its implementation variations are explained as follows;

Single code generation implementation.

An approval code is generated by the credit card issuer and is either sent directly to the cardholder's UID or made available to the cardholder through a secure channel of distribution such as a web site. The cardholder enters the code when the merchant's system prompts for it. When the code has been entered in the merchant's system, it is sent to the credit card issuer for comparison. The credit card issuer carries out comparison of the approval codes. Code generation does not take place on the merchant's system. This alternative is shown in detail in Figs 1.a 1.c.

Shopper check-code generation implementation.

Code generation takes place both on the credit card issuer's system and on the cardholder's UID, which, in this alternative, must be capable of storing and executing a program. The code generated by the UID is requested by the merchant

system as part of the information necessary to initiate a transaction. This approval code is then sent to the credit card issuer for comparison of the codes. This alternative is shown in detail in Figs 2.a-2.c.

Merchant check-code generation implementation.

Code generation takes place on both the credit card issuer's system and the merchant's system. The approval code generated by the credit card issuer is sent to the cardholder's UID. The merchant's system is responsible for comparison of the codes. This alternative is shown in detail in Figs 3.a-3.c.

Single code generation implementation in detail.

Accompanying figures

1.a Flow of information in a legitimate transaction
1.b Flow of information in an attempted fraudulent use
1.c System Flowchart

In this scenario, the credit card issuer does not verify the identity of the shopper unless the merchant site sends an approval code. An approval code is generated by the credit card issuer's system. This code may either be sent directly to the credit cardholder's UID or made available on demand to the credit card holder. The cardholder then provides the merchant with the approval code. In the case where the shopper is the actual cardholder they will be able to provide the correct code but if the shopper is not the cardholder then they will not be able to provide the approval code.

The merchant system sends the approval code received from the shopper to the credit card issuer. The credit card issuer receives and compares the two approval codes (Credit card issuer generated approval code and merchant sent approval code). If the codes match each other then the credit card issuer verifies the identity of the shopper, approves the order and notifies the merchant.

The scenarios below describe the processes involved in a legitimate transaction and in a case of attempted fraudulent use. The examples use e-commerce as a context but the same processes would apply in any transaction.

The actual cardholder initiates the credit card transaction and the credit card issuer is method-enabled. The merchant's web site has been modified to handle the method and system (Fig. 1.a):

Step 1- During a typical on-line purchase; the credit card holder (shopper) completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to merchant's site.

Step 2 - The shopper's credit card data is sent for authorization by the credit card issuer.

Step 3 - The credit card issuer checks the incoming data sent by the merchant. The credit card is then authorized. The transaction itself is not yet completed. An approval code is generated by the credit card issuer's system. This code is either sent to the UID of the cardholder or made available to them on demand. The credit card issuer may have obtained the cardholder's UID access data previously.

Step 4- The merchant asks for an approval code field to be filled in by the shopper. To complete the transaction the shopper enters the approval code.

Step 5- The merchant site sends the approval code supplied by the shopper to the credit card issuer for comparison.

Step 6- The credit card issuer checks the incoming code and verifies the identity of the shopper. The credit card issuer then sends the approval confirmation to the merchant.

The credit card transaction is initiated by an unauthorized shopper (fraudulent card use) and the credit card issuer is method enabled. The merchant's web site has been modified to handle the method and system (Fig. 1.b):

Step 1 - During a typical on-line purchase the shopper completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to the merchant's site.

Step 2 - The shopper's credit card data is sent for authorization by the credit card issuer.

Step 3 - The credit card issuer checks the incoming data sent by the merchant. The credit card is then authorized for use. The transaction itself is not yet completed. An approval code is generated by the credit card issuer's system. This code is either sent to the UID of the cardholder or made available to them on demand. The credit card issuer may have obtained the cardholder's UID access data previously. If the approval code has been sent to the cardholder's UID then the cardholder is aware that a third party is attempting to carry out a transaction using their credit card and can respond by contacting the credit card issuer. This contact may be facilitated by a 'reply' functionality included in the approval code messages that are sent to the cardholder's UID. When the cardholder receives the approval code message they can reply to it, usually using a built in function of their UID. The originator of the message would then receive the reply and could act on it by triggering an alarm message or procedure. The ultimate aim of the 'reply' functionality is to automate the process of informing a credit card issuer that attempted fraudulent use of a card is taking place.

Step 4 - The merchant asks for an approval code field to be filled in by the shopper. The shopper, who is not the cardholder, has not received the approval code and cannot supply it.

Step 5 - The merchant site sends either no approval code or an incorrect code supplied by the shopper to the credit card issuer for comparison.

Step 6 - The credit card issuer checks the incoming code and cannot verify the identity of the shopper. Credit card issuer then informs the merchant that approval for the transaction cannot be given.

Flowchart, refer to Fig. 1.c;

Merchant:

In step 4100 and 4101, the information entered by the shopper is validated.
In step 4102, the validated customer data by the merchant site is sent to the credit card processor for data processing and routing for credit card authorization. The information is sent to credit card issuer by the credit card processor or similar organizations in the following step 4300.
In step 4103, the result of the authorization request is received from the credit card issuer.
In step 4104, the authorization message from the credit card issuer is evaluated. If authorization is obtained then step 4106 is processed, otherwise step 4110 is processed.
In step 4106, the merchant site receives the approval code entered by the shopper.
In step 4109, the shopper data along with the approval code entered by the shopper is communicated to the credit card issuer for approval. At this moment, the order has not been approved by the credit card issuer.
In step 4110, the merchant system informs the shopper that the transaction has either not been authorized or not been approved.
In step 4111, the merchant site gets the final purchase approval from the credit card issuer.
In step 4112, the credit card issuer's response is evaluated. If the credit card issuer has approved the order then step 4113 is performed. Otherwise, the step 4110 is processed.
In step 4113, the credit card issuer has approved the order. The merchant informs the shopper about the purchase order approval.

The Shopper:

In step 4200, the shopper enters all the information requested by the merchant's site. Figure 4 shows the information requested by the merchant to process and validate the credit card.
In the steps 4201 and 4202 the shopper/cardholder receives the approval code and enters it into the merchant site.
Only the cardholder can obtain the approval code. Shoppers who are not cardholders will not receive the correct approval code.

Credit Card Processor:

In steps 4300 and 4303, the credit card processor receives the data in a predetermined format, processes it and then routes it to the destination for further processing and authorization. At this stage, the merchant supplied data is handled by the credit card processor and communicated to the credit card issuer. The credit card processor and other intermediary organizations use different versions of VPOS software and systems to process credit card authorization requests. The procedures are similar but may display some variations depending on the credit card association and the different countries involved.

The Credit Card Issuer:

In step 4401, the credit card issuer receives the credit card authorization request and processes it using the credit card customer data it possesses according to the procedures and rules established by the credit card associations and the countries involved in the particular transaction.
In step 4402, the credit card issuer receives the data from the merchant for first authorization. If the credit card is not authorized then this information is passed to the merchant (step 4301). If the credit card is authorized then step 4403 is processed.
In step 4403, authorization information is sent to the merchant by step 4301.
In step 4404, the credit card issuer generates an approval code that is sent to the cardholder's UID. The UID access information is in the credit card issuer's database and it has been obtained by the bank during initial card issuing process.
In step 4405, The shopper data along with the approval code entered by the shopper is communicated to the credit card issuer for final approval.
In step 4406, the approval code received from the merchant entered by the shopper and the one generated by the credit card issuer are compared. If the approval codes match then the identity of the shopper is verified and step 4407 is performed. If they do not match then step 4408 is processed.
In step 4407, the transaction is approved. Merchant is notified via step 4303.
In step 4408, the credit card issuer does not approve the transaction and sends this information to the merchant via step 4303.

POS processing for single code generation implementation.

The invention applies to traditional credit card purchases as well as on-line, mail order or telephone "card not present" transactions. During a traditional credit card purchase, merchants use a physical POS device to swipe the credit card. Most current POS devices are equipped with a keypad. In order to apply the invention to regular POS processing, all the merchant system is required to have is a shopper interface that accepts approval codes (sent by the credit card issuer to shopper's UID) and communicates them to the credit card issuer. This interface may use the regular POS device or merchant supplied secure data entry device. If the correct approval code cannot be sent to the credit card issuer in a predefined period of time then the

credit card issuer cancels the approval process and the entire process needs to be started from the beginning. The merchant swipes the card through the POS device. The credit card issuer authorizes the transaction but does not approve the order at this time. An approval code is generated by the credit card issuer and sent to the UID of the cardholder. The cardholder is standing by the POS device and expecting to receive an approval code via his/her UID. The message comes to the UID of the cardholder. The cardholder enters the approval code by using merchant provided interface (i.e., POS device's own buttons). The approval code is sent to the credit card issuer. The credit card issuer compares the codes to verify the identity of the shopper and either approves the order or not. This logic makes the system extremely secure since each code generated is unique and for one-time use only.

Shopper check-code generation implementation.

Accompanying figures

2.a Flow of information in a legitimate transaction
2.b Flow of information in an attempted fraudulent use
2.c System flowchart

In this second scenario, the cardholder's UID is a programmable device and is capable of generating an approval code. Both the credit card issuer and the cardholder's UID generate approval codes. In order for these codes to match both code generation processes need access to the code generation key. Figure 5 illustrates the method by which approval codes are generated with or without the use of code generation keys. The code generation key is an alphanumeric code used to verify the identity of an individual attempting to use a credit card, debit card, or other account. The code generation key is assigned by the credit card issuer or chosen by the cardholder and accessible only by the credit card issuer and the cardholder.

Another factor used in the generation of an approval code is a time/date value. The use of a time/date value ensures that the value generated as an approval code will be time sensitive. Approval codes will, therefore, have a limited lifespan. The length of this lifespan can be varied to meet the demands of the specific implementation. In one implementation, for example, the lifespan of the approval code could be set to 15 minutes, ensuring that a code generated at 9:00am would cease to be valid at 9:16am.

In order to avoid localization issues and ensure that approval codes generated in different locations match, all systems involved in a transaction should base their generation of approval codes on an agreed time-zone and make an adjustment for their local time zone before carrying out a comparison of approval code values. In a transaction for a shopper in Istanbul (GMT +2), purchasing goods or services from a merchant in London, using a card issued by a credit card issuer in New York (GMT -5), three different time zones may be involved. Any time-based input into approval code generation would need to be based on a single time zone. If GMT is the agreed

standard then systems in Istanbul would use local time –2 and systems in the USA would use local time + 5.

The scenarios below describe the processes involved in a legitimate transaction and in a case of attempted fraudulent use. The examples use e-commerce as a context but the same processes would apply in any transaction.

The actual cardholder initiates the credit card transaction and the credit card issuer is method-enabled. The merchant's web site has been modified to handle the method and system (Fig. 2.a):

Step1 - During a typical on-line purchase the credit cardholder (shopper) completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to the merchant's site. In this step, an approval code is specifically requested by the merchant system. The shopper enters the approval code generated by his/her UID.

Step 2 - The merchant sends the data required for approval (including the approval code entered by the shopper) to the credit card issuer.

Step 3 - the credit card issuer generates an approval code. This approval code is compared with the approval code sent by the merchant. If the credit card information is correct and the approval codes match then the transaction is approved by the credit card issuer and the merchant is notified of the approval.

The credit card transaction is initiated by an unauthorized shopper (fraudulent card use) and the credit card issuer is method enabled. The merchant's web site has been modified to handle the method and system (Fig. 2.b) :

Step 1 - During a typical on-line purchase the shopper completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to the merchant's site. In this step an approval code is specifically requested by the merchant's system. As the shopper is not the actual cardholder, the approval code generated by the cardholder's UID cannot be accessed by the shopper. The shopper either does not enter an approval code or enters an incorrect approval code.

Step 2 - The merchant sends the data to the credit card issuer.

Step 3 - the credit card issuer generates an approval code. This approval code is compared with the approval code sent by the merchant. The approval codes will not match, since the actual approval code cannot be accessed by the shopper. The credit card issuer does not approve the transaction request. Credit card issuer then sends the result of the approval request as not approved to the merchant.

Flowchart, refer to Fig. 2.c;

Merchant:

In step 5100 and 5101, the information entered by the shopper is validated.
In step 5102, the validated customer data is sent by the merchant site to the credit card processor for data processing and routing for credit card authorization. The information is sent to the credit card issuer by the credit card processor or similar organizations in the following step 5300. This information also contains the approval code entered by the shopper.
In step 5110, the merchant system warns the shopper that the transaction is not approved and stops the processing of the purchase request.
In step 5111, the merchant site gets the final purchase approval from the credit card issuer.
In step 5112, the credit card issuer's response is evaluated. If the credit card issuer has approved the order then the step 5513 is performed. Otherwise, the step 5110 is processed.
In step 5513, the credit card issuer has approved the order. The merchant informs the shopper about the purchase order approval.

The Shopper:

In step 5200, the shopper enters all the information requested by the merchant's site. Figure 4 shows the information requested by the merchant to process and validate the credit card. In this step, an approval code is specifically requested by the merchant system.
In step 5203, the shopper is informed that the transaction has not been approved.
In step 5204, the shopper is informed that the transaction has been approved.

Credit Card Processor:

In steps 5300 and 5303, the credit card processor receives the data in a predetermined format, processes it and then routes it to the destination for further processing and authorization. At this stage, the merchant supplied data is handled by the credit card processor and communicated to the credit card issuer. The credit card processor and other intermediary organizations use different versions of VPOS software and systems to process credit card authorization requests. The procedures are similar but may display some variation depending on the credit card association and the different countries involved.

The Credit Card Issuer:

In step 5401, the credit card issuer receives the credit card approval request and processes it using the credit card customer data it possesses according to the procedures and rules established by the credit card associations and the countries involved in the particular transaction.
In step 5404, the credit card issuer generates an approval code.

In step 5406, the approval code received from the merchant and the one generated by the credit card issuer are compared. If the approval codes match, step 5407 is performed. If not, then step 5408 is processed.
In step 5407, the transaction is approved. Merchant is notified via step 5303.
In step 5408, the credit card issuer does not approve the transaction and sends this information to the merchant via step 5303.

POS processing for shopper check-code generation.

The invention applies to traditional credit card purchases as well as on-line, mail order or telephone "card not present" transactions. During a traditional credit card purchase, merchants use a physical POS device to swipe the credit card. Most recent POS devices are equipped with a keypad. In order to apply the invention to regular POS processing, all the merchant system is required to have is a shopper interface that accepts approval codes (generated by the shopper's UID) and communicates them to the credit card issuer. This interface may use the regular POS device or merchant supplied secure data entry device. If the correct approval code cannot be sent to the credit card issuer in a predefined period of time then the credit card issuer cancels the approval process and the entire process needs to be started from the beginning. The merchant swipes the card through the POS device. The credit card issuer authorizes the transaction but does not approve the order at this time. An approval code is generated by the cardholder's UID. The cardholder enters the approval code by using merchant provided interface (i.e., POS device's own buttons). The approval code is sent to the credit card issuer. The credit card issuer compares the codes to verify the identity of the shopper and either approves the order or not. This logic makes the system extremely secure since each code generated is unique and for one-time use only.

Merchant check-code generation implementation.

Accompanying figures

3.a Flow of information in a legitimate transaction
3.b Flow of information in an attempted fraudulent use
3.c System flowchart

In this third scenario, the approval code generation may take place on both the merchant and the credit card issuer's system. The comparison of codes must take place on the merchant's system.

When a shopper wishes to make a purchase using a credit card they supply their credit card data to the merchant system. This information may or may not include a code generation key. The merchant system will sent the credit card related information to the credit card issuer for authorization. If a code generation key is supplied it will be used to generate an approval code.

The credit card issuer receives the information supplied by the merchant and either authorizes or declines the transaction request. If the request is authorized and the card is protected by the invention then the credit card issuer generates an approval code and sends it to the UID of the cardholder.

If the credit card issuer authorizes the transaction and the shopper has provided a code generation key then the shopper will be prompted by the merchant to enter the approval code sent to their UID by the credit card issuer. The merchant can then make the comparison between the code it has generated and the code entered by the shopper. The transaction is either verified and approved or declined.

The table below shows the possible combinations of processes that characterize a credit card transaction based on merchant and credit card issuer's status.

No	Invention Enabled	Not Invention Enabled	RESULT
1	Merchant Credit Card Issuer		The identity of the shopper is verified as the authorized user of the credit card. If the shopper is attempting to use the card fraudulently and does not enter a code generation key then the cardholder is made aware of this fraudulent use by the approval code being sent to their UID. If the shopper enters an incorrect code generation key then the transaction is not approved.
2	Credit Card Issuer	Merchant	The invention will inform the cardholder if attempted fraudulent credit card use is in progress. Although the credit card issuer may authorize the transaction the cardholder can inform the Issuer as soon as the approval code is received by their UID.
3		Merchant Credit Card Issuer	Transaction proceeds using current authorization process.
4	Merchant	Credit Card Issuer	Shopper will not provide a code generation key. Transaction proceeds using current authorization process.

The scenarios below describe the processes involved in legitimate transactions and in cases of attempted fraudulent use. The examples use e-commerce as a context but the same processes would apply in any transaction.

The credit card transaction is initiated by the actual cardholder and the credit card issuer is method-enabled (Fig.3.a):

Step1 - During a typical on-line purchase the credit cardholder (shopper) completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to the merchant's site. The merchant specifically requests a code generation key from the shopper. The shopper is the cardholder and has access to this key.

Step 2 - The merchant sends the data required for authorization to the credit card issuer.

Step3 - The credit card issuer authorizes the transaction, allocates funds for transfer to the merchant's account and generates an approval code which is sent to the cardholder's UID.

Step 4 - Because the shopper has provided a code generation key the merchant prompts the shopper for an approval code. The shopper enters the approval code sent by the credit card issuer to his/her UID. The merchant compares the approval codes, verifies the identity of the shopper and approves the transaction.

The actual cardholder initiates the credit card transaction and the credit card issuer is not method-enabled (Fig. 3.a):

Step 1 - During a typical on-line purchase the credit cardholder (shopper) completes the selection of products or services over the e-commerce site. The shopper then enters his/her credit card data along with other personal information such as address, etc. to the merchant's site. The merchant specifically requests a code generation key from the shopper. The shopper does not have access to a code generation key because their credit card issuer has not provided them with one. The shopper leaves this field blank.

Step 2 - The merchant sends the data required for authorization to the credit card issuer.

Step 3 - The credit card issuer authorizes the transaction and allocates funds for transfer to the merchant's account. No approval code is generated as the credit card issuer is not using the invention.

Step 4 - The merchant does not prompt the shopper for an approval code as no code generation key has been provided. The transaction is complete. This transaction is uneffected by the invention.

The credit card transaction is initiated by an unauthorized shopper (fraudulent card use) and the credit card issuer is method-enabled (Fig. 3.b): (Fig. 3.b)

Step 1 - During a typical on-line purchase the shopper (unauthorized) completes the selection of products or services over the e-commerce site. The shopper then enters the cardholder's credit card data along with other personal information such as address, etc. to the merchant's site. The merchant specifically requests a code generation key from the shopper. The shopper does not have access to the cardholder's code generation key. The shopper may enter an incorrect key or leave the field blank.

Step 2 - The merchant sends the data required for authorization to the credit card issuer.

Step 3. The credit card issuer authorizes the transaction, allocates funds for transfer to the merchant's account and generates an approval code, which is sent to the cardholder's UID.

Step 4. If the shopper has provided a code generation key then the merchant site will prompt them for an approval code. This code is only available through the cardholder's UID and the shopper will not be able to obtain the code. In this case the merchant will not complete the transaction. If the shopper has not provided a code generation key then the merchant site will not prompt for an approval code and will complete the transaction. In either case the cardholder is made aware that a third party is attempting to carry out a transaction using their credit card and can respond by contacting the credit card issuer. This contact may be facilitated by a 'reply' functionality included in the approval code messages that are sent to the cardholder's UID. When the cardholder receives the approval code message they can reply to it, usually using a built in function of their UID. The originator of the message would then receive the reply and could act on it by triggering an alarm message or procedure. The ultimate aim of the 'reply' functionality is to automate the process of informing a credit card issuer that attempted fraudulent use of a card is taking place.

The credit card transaction is initiated by an unauthorized shopper (fraudulent card use) and the credit card issuer is not method-enabled (Fig. 3.b):

Step 1 - During a typical on-line purchase the shopper (unauthorized) completes the selection of products or services over the e-commerce site. The shopper then enters the cardholder's credit card data along with other personal information such as address, etc. to merchant's site. The merchant specifically requests a code generation key from the shopper. The shopper does not have access to the cardholders code generation key. The shopper may enter an incorrect key or leave the field blank.

Step 2. The merchant sends the data required for authorization to the credit card issuer.

Step 3. The credit card issuer authorizes the transaction and allocates funds for transfer to the merchant's account.

Step 4. The merchant site receives the authorization from the credit card issuer. The transaction is complete. This transaction is uneffected by the invention.

Flowchart, refer to Fig. 3.c;

The Merchant:

In step 3100 and 3101, the information entered by the shopper is validated.
In step 3102, the validated customer data is sent by the merchant site to the credit card processor for data processing and routing for credit card authorization. The information is sent to the credit card issuer by the credit card processor or similar organizations in step 3300.
In step 3103, the authorization result is received from the credit card issuer
In step 3104, the authorization result from the credit card issuer is evaluated
In step 3105, if the transaction is not authorized then the merchant site informs the shopper about this failure. If the transaction is authorized then step 3107 is processed.
In step 3107, an evaluation is performed to determine whether the shopper has provided a code generation key. If no code generation key has been provided then step 3112 is performed. Step 3112 represents the normal conclusion of a credit card transaction without the protection of the invention. If the shopper has provided a code generation key then step 3108 is processed
In step 3108, an approval code is generated using the code generation key provided by the shopper.
In step 3109, the merchant site receives the approval code entered by the shopper.
In step 3110, the code generated by the merchant site and the code entered by the shopper are checked to determine if they match. If the codes are the same then the order is accepted and the step 3113 will be processed. If the approval codes do not match then the merchant is aware that the identity of the shopper has not been verified. The merchant may either accept the order and ship the products, accepting the risk that the credit card issuer may revoke the transaction at a later date (NO 1), or refuse to accept the order and cancel the transaction by communicating with the credit card issuer (NO 2).

The Shopper:

In step 3200, the shopper enters all the information requested by the merchant's site. Figure 4 shows the information requested by the merchant to process and validate the credit card. The shopper is also asked to provide a code generation key.
In steps 3201, the shopper receives the approval code sent to the cardholders UID by the credit card issuer.
In step 3202, the approval code is provided to the merchant site by the shopper.
The shopper can obtain the approval code only if the shopper is the cardholder. If the cardholder receives an approval code for a transaction they have not initiated they are made aware that a third party is attempting to carry out a transaction using their credit card and can respond by contacting the credit card issuer. This contact may be facilitated by a 'reply' functionality included in the approval code messages that are sent to the cardholder's UID. When the cardholder receives the approval code message they can reply to it, usually using a built in function of their UID. The originator of the message would then receive the reply and could act on it by triggering an alarm message or procedure. The ultimate aim of the 'reply'

functionality is to automate the process of informing a credit card issuer that attempted fraudulent use of a card is taking place.

Credit Card Processor:

In steps 3300 and 3301, the credit card processor receives the data in a predetermined format, processes it and then routes it to the destination for further processing and authorization. At this stage, the merchant supplied data is handled by the credit card processor and communicated to the credit card issuer. The credit card processor and other intermediary organizations use different versions of VPOS software and systems to process credit card authorization requests. The procedures are similar but may display some variations depending on the credit card association and the different countries involved.

The Credit Card Issuer:

In step 3400 and step 3401, the credit card issuer receives the credit card authorization request and processes it using the credit card customer data according to the procedures and rules established by the credit card associations and the countries involved in the particular transaction.
In step 3401, if the credit card is not authorized then this information is passed to the merchant via steps 3301. If the credit card issuer authorizes the credit card this information is also passed to the merchant following the same steps.
In step 3402, if the credit card issuer is protected by the invention then step 3403 is processed and an approval code is sent to the cardholders UID in Step 3301.
In step 3403, the credit card issuer generates an approval code. This approval code is sent to the cardholder's UID. But in this step the credit card issuer is not sure whether the approved purchase is fraudulent or not even if the card has authorized.

LOOK UP SERVER OPTION

In the above scenarios the merchant cannot identify whether or not an individual credit card is protected by the invention. In order to make the system more effective a look up server can be added. The role of a look up server is described in Fig. 6. By including a look up server in the invention configuration, the merchant becomes aware whether the credit card submitted in the purchase request is protected by the invention or not.

The look up server maintains receives a query from a merchant containing the first 'n' digits of a credit card number where 'n' is the number of digits necessary to identify the credit card issuer and the type of credit card in use. These digits do not represent individual credit cards. The look up server maintains a list of these partial credit card numbers, which is added to whenever a new type of credit card is protected using the invention. The look up server can respond to the merchant with a value indicating that the type of card is either protected by the invention or is not. The

merchant then proceeds with knowledge of the credit card's protection status. This knowledge allows the merchant to refuse to process transactions from cards protected by the invention without the presentation of either

I. A Code Generation Key
II. An Approval Code
III. Both

If the shopper does not provide the required information then the merchant can halt processing of the transaction at that point.

CLAIMS

1. A method and system for preventing credit card fraud comprising the steps of:

the credit cardholder provides the merchant with the information necessary for credit card authorization;
the credit card issuer receives the credit card specific information obtained by the merchant;
the credit card issuer processes the credit card for authorization ;
if the credit card is authorized then the credit card issuer generates an approval code and this approval code is sent to the unique identification device (UID) of the cardholder using a communication network;
the credit card issuer communicates the authorization decision to the merchant;
the merchant prompts the cardholder to supply an approval code;
the cardholder supplies the approval code they have received via their unique identification device (UID);
the merchant sends the approval code presented by the shopper to the credit card issuer;
the credit card issuer compares the approval code it has generated with the approval code sent by the merchant;
the credit card issuer approves the credit card transaction only if the approval codes match.

2. A method and system for preventing credit card fraud comprising the steps of:

the credit cardholder provides the merchant with the information necessary for credit card authorization;
the credit card issuer receives the credit card specific information obtained by the merchant;
the credit card issuer processes the credit card for authorization;
if the credit card is authorized then the credit card issuer generates an approval code, which is made available to the cardholder in a mutually agreed protected environment;
the credit card issuer communicates the authorization decision to the merchant;
the merchant prompts the cardholder to supply an approval code;
the cardholder retrieves the approval code from the mutually agreed protected environment;
the cardholder supplies the merchant with the approval code they have retrieved;
the merchant sends the approval code presented by the shopper to the credit card issuer;
the credit card issuer compares the approval code it has generated with the approval code sent by the merchant;

the credit card issuer approves the credit card transaction only if the approval codes match.

3. A method and system for preventing credit card fraud comprising the steps of:

the credit cardholder provides the merchant with the information necessary for credit card authorization;
the cardholder uses their unique identification device (UID) to generate an approval code based on the code generation key associated with their credit card; where code generation key is an alphanumeric code used to verify the identity of the cardholder and it is accessible only by the credit card issuer and the cardholder;
the cardholder provides the merchant with this approval code;
the merchant sends the credit card specific information with the approval code to the credit card issuer;
the credit card issuer receives the information sent by the merchant;
the credit card issuer processes the credit card for authorization;
if the credit card is authorized then the credit card issuer generates an approval code based on the code generation key associated with the credit card;
the credit card issuer compares the approval code it has generated with the approval code sent by the merchant; the credit card issuer approves the credit card transaction only if the approval codes match.

4. A method and system for preventing credit card fraud comprising the steps of:

the credit cardholder provides the merchant with the information necessary for credit card authorization;
the credit cardholder provides the merchant with the code generation key associated with their credit card; where code generation key is an alphanumeric code used to verify the identity of the cardholder and it is accessible only by the credit card issuer and the cardholder;
the credit card issuer receives the credit card specific information obtained by the merchant;
the credit card issuer processes the credit card for authorization ;
if the credit cardholder has provided a code generation key and the transaction has been authorized by the credit card issuer then the following additional steps take place:
the credit card issuer generates an approval code using the code generation key associated with the credit card and this approval code is sent to the unique identification device (UID) of the cardholder using a communication network;
the credit card issuer communicates the authorization decision to the merchant;
the merchant generates an approval code based on the code generation key provided by the credit cardholder;

the merchant prompts the credit cardholder to supply the approval code that has been received from the credit card issuer via the cardholder's unique identification device (UID);
the merchant compares the approval code it has generated with the approval code provided by the cardholder;
the result of the comparison allows the merchant to make a decision regarding the legitimacy of the transaction.

5. A communication component referred to as Unique Identification Device (UID) in the method of claims 1,4 is a device that is capable of receiving messages.

6. A communication component referred to as Unique Identification Device (UID) in the method of claims 1,4 is a device that is capable of receiving and sending messages.

7. A communication component referred to as Unique Identification Device (UID) in the method of claims 5, 6 is a mobile phone.

8. A communication component referred to as Unique Identification Device (UID) in the method of claims 5, 6 is an e-mail account.

9. A communication component referred to as Unique Identification Device (UID) in the method of claims 5, 6 is a wireline phone (or Phone Number??).

10. A communication component referred to as Unique Identification Device (UID) in the method of claims 5, 6 is a wireless phone.

11. A communication component referred to as Unique Identification Device (UID) in the method of claims 5,6 is a pager device.

12. A communication component referred to as Unique Identification Device (UID) in the method of claims 5,6 is a personal computer.

13. A communication component referred to as Unique Identification Device (UID) in the method of claims 5,6 is a personal digital assistant (pda) device.

14. A communication component referred to as UID in the method of claim 3 is a device that is capable of generating approval code.

15. A communication component referred to as UID in the method of claim 14 is a personal computer.

16. A communication component referred to as UID in the method of claim 14 is a personal digital assistant (pda).

17. A communication component referred to as UID in the method of claim 14 is a mobile phone.

18. A communication component referred to as UID in the method of claim 14 is a pager device.

19. A communication component referred to as UID in the method of claim 14 is an electronic organizer device.

20. A method as in claims 3 and 4 of generating an alphanumeric code using a Code Generation Key and an adjusted date/time stamp where the adjustment of date/time stamps is based on a time-zone agreed on as a point of reference by all systems involved in the processes of generating or comparing approval codes.

21. A method as in claims 1, 2, 3, 4 of enabling the merchant, in a credit card transaction, to ascertain whether an individual credit card is protected by the method and system through reference to a 'look up' server containing records of all types of credit cards protected by the method and system.

22. The method of claims 1, 4 wherein the cardholder is informed, via their UID, of attempted fraudulent use of their credit card account by a third party.

23. The method of claim 22 wherein the cardholder notifies their credit card issuer of attempted fraudulent use by replying to a message received via their UID.

24. The method of claim 23 where the reply mechanism is a return e-mail address on an email message containing the approval code generated by the credit card issuer.

25. The method of claim 23 where the reply mechanism is an originating GSM number on a GSM SMS message containing the approval code generated by the credit card issuer.

26. The method of claim 23 where the reply mechanism is a telephone number that connects to an automatic call directing service.

27. The method of claim 24 where the reply mechanism is a website.

Figure 1.a

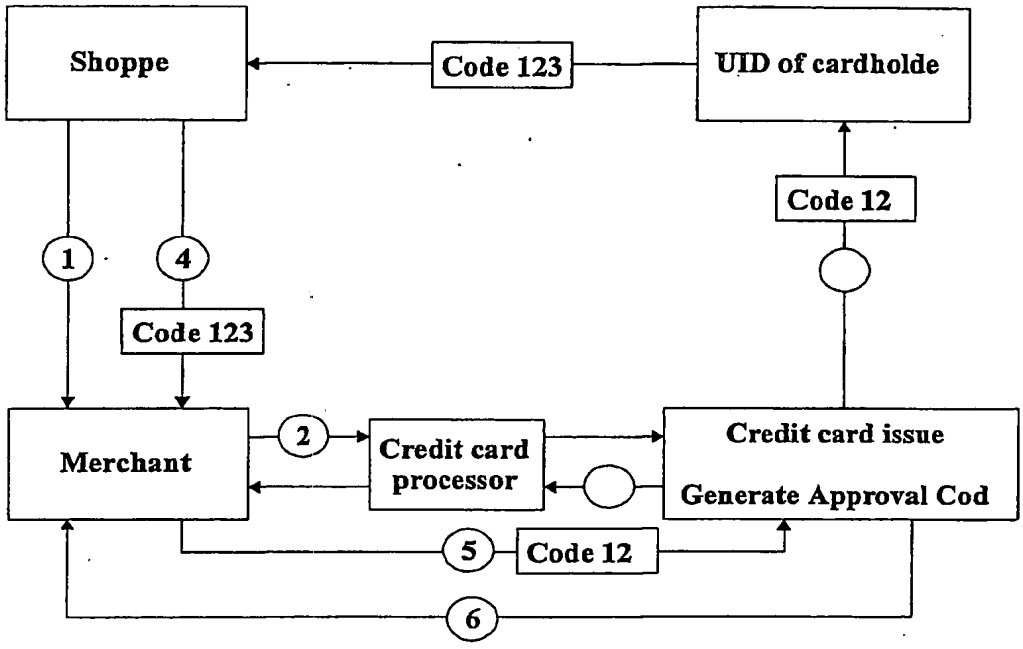


Figure 1.b

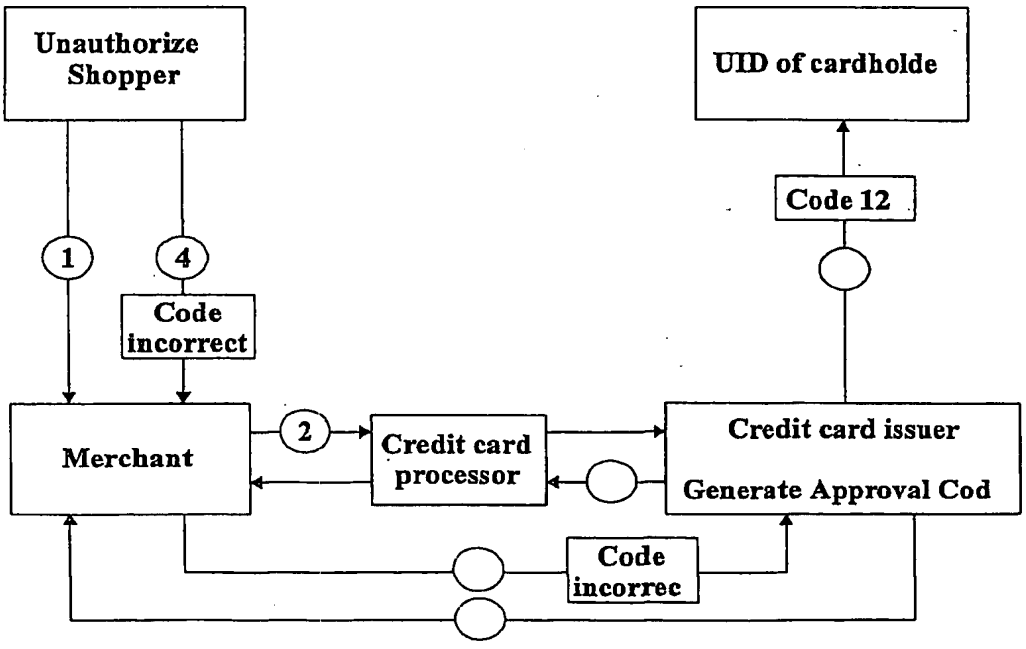


Figure 1.c

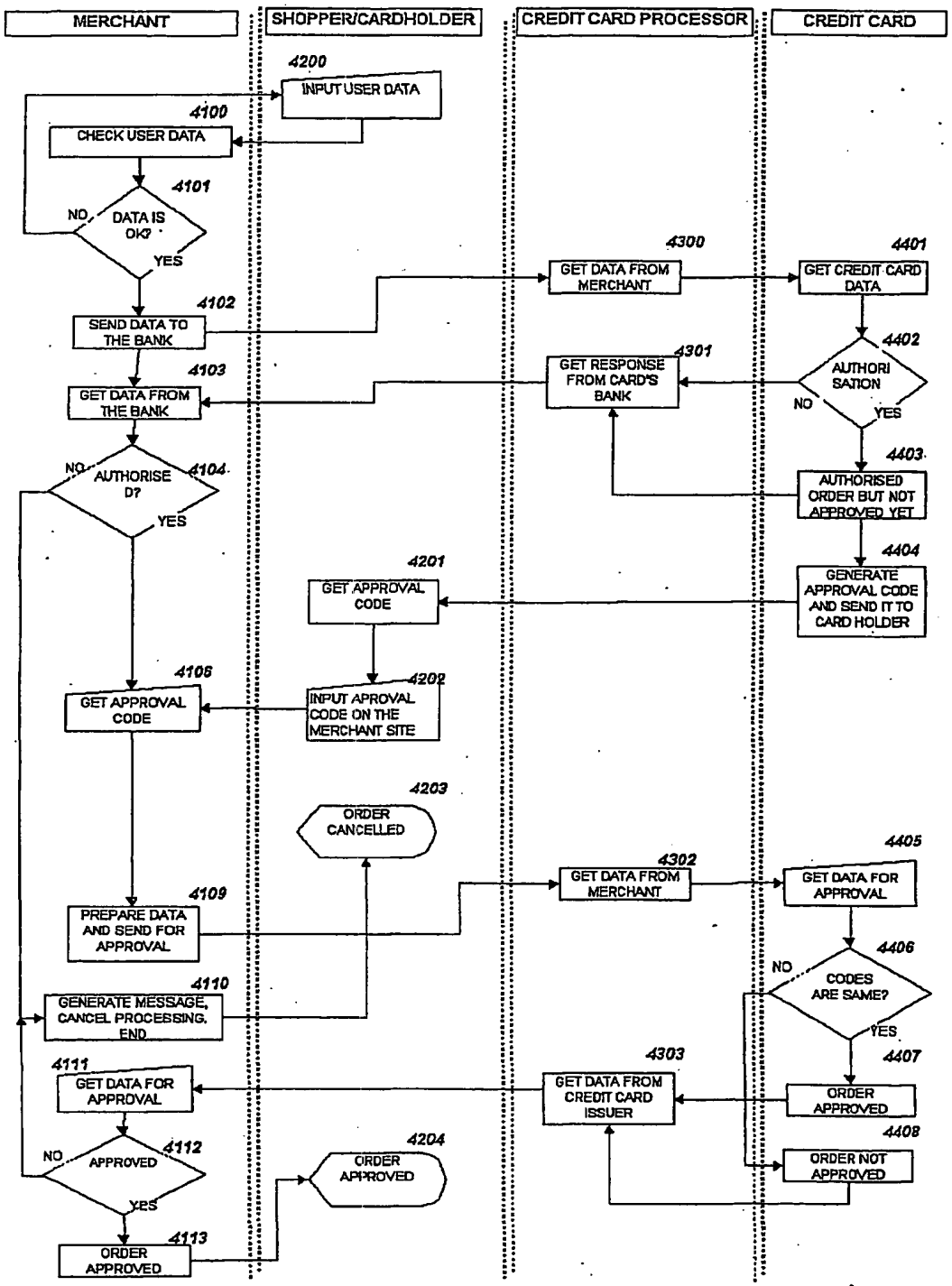

MERCHANT
SHOPPER/CARDHOLDER
CREDIT CARD PROCESSOR
CREDIT CARD
4200
INPUT USER DATA
4100
CHECK USER DATA
4101
DATA IS OK?
NO
YES
4102
SEND DATA TO THE BANK
4103
GET DATA FROM THE BANK
AUTHORISED?
4104
NO
YES
4106
GET APPROVAL CODE
4109
PREPARE DATA AND SEND FOR APPROVAL
4110
GENERATE MESSAGE, CANCEL PROCESSING, END
4111
GET DATA FOR APPROVAL
APPROVED?
4112
NO
YES
4113
ORDER APPROVED
4203
ORDER CANCELLED
4204
ORDER APPROVED
4201
GET APPROVAL CODE
4202
INPUT APROVAL CODE ON THE MERCHANT SITE
4300
GET DATA FROM MERCHANT
4301
GET RESPONSE FROM CARD'S BANK
4302
GET DATA FROM MERCHANT
4303
GET DATA FROM CREDIT CARD ISSUER
4401
GET CREDIT CARD DATA
4402
AUTHORISATION
NO
YES
4403
AUTHORISED ORDER BUT NOT APPROVED YET
4404
GENERATE APPROVAL CODE AND SEND IT TO CARD HOLDER
4405
GET DATA FOR APPROVAL
4406
CODES ARE SAME?
NO
YES
4407
ORDER APPROVED
4408
ORDER NOT APPROVED

Figure 2.a

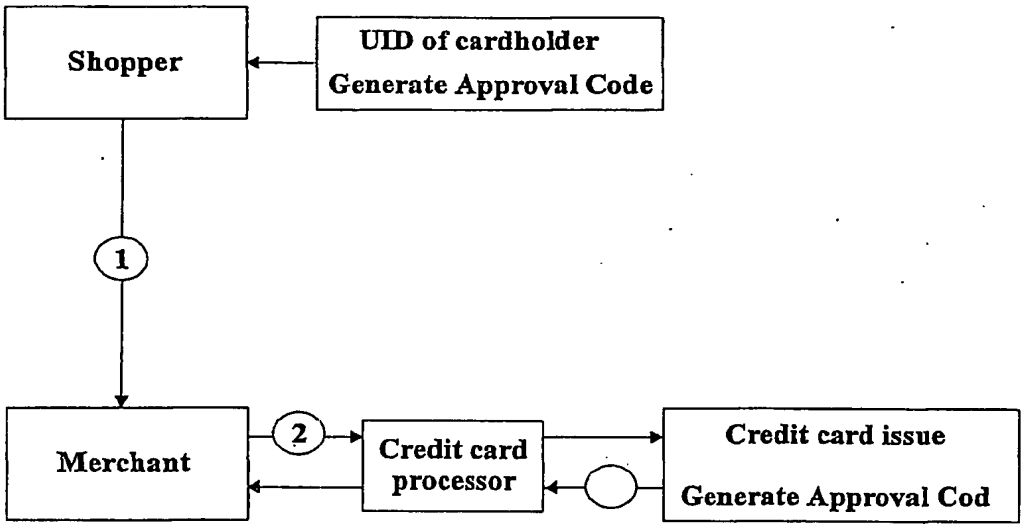


Figure 2.b

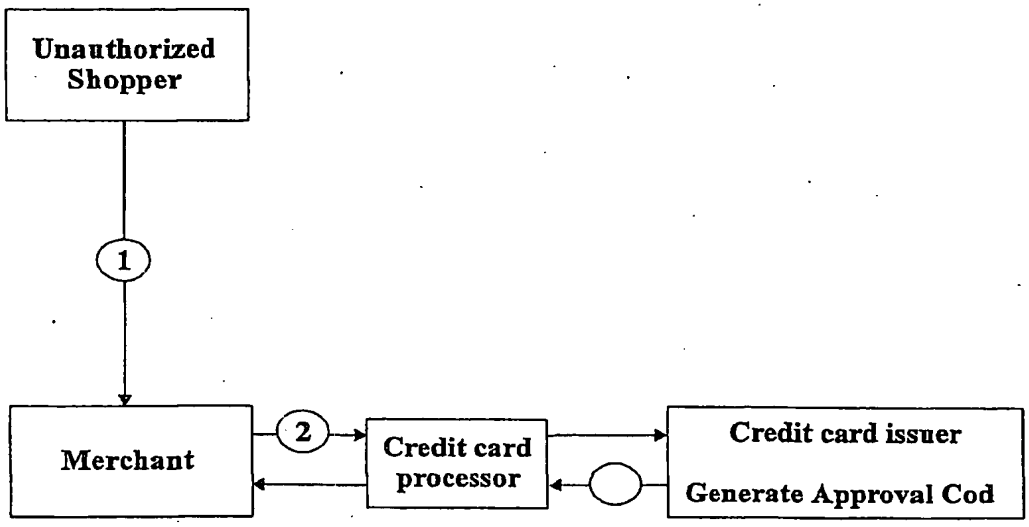


Figure 2.c

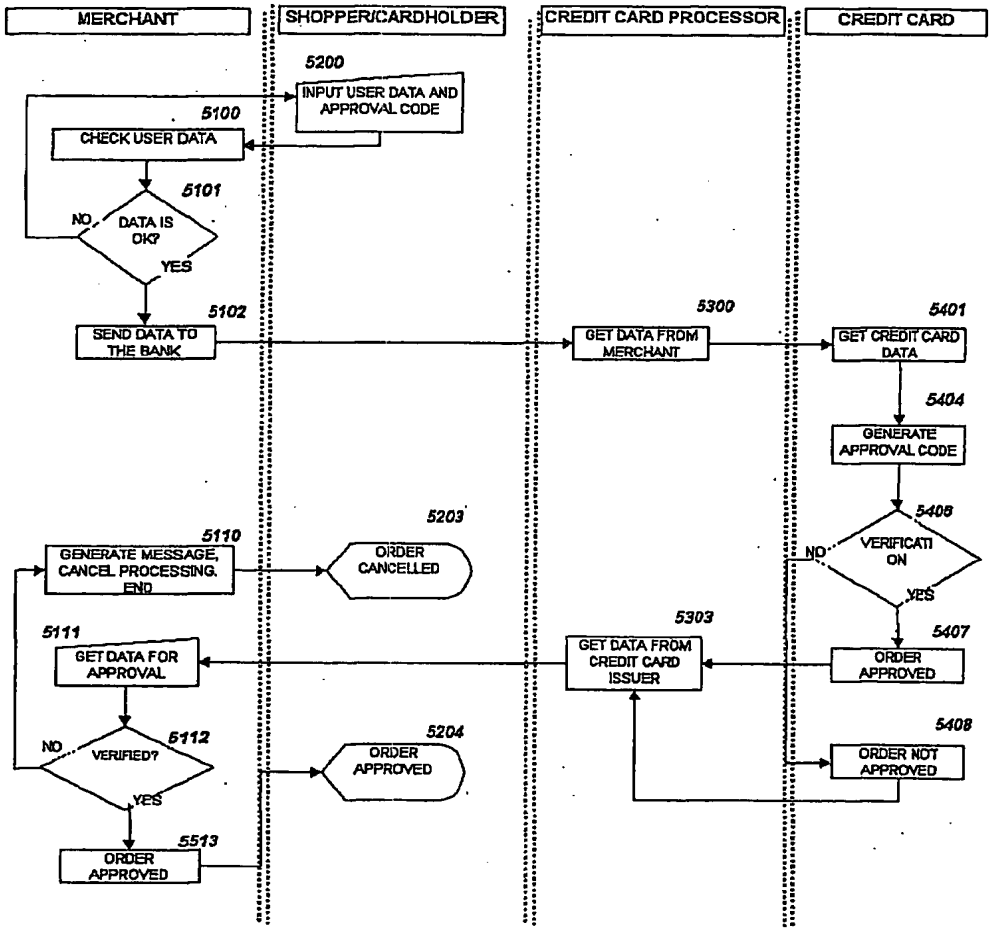

MERCHANT
SHOPPER/CARDHOLDER
CREDIT CARD PROCESSOR
CREDIT CARD
5200
INPUT USER DATA AND APPROVAL CODE
5100
CHECK USER DATA
5101
DATA IS OK?
NO
YES
5102
SEND DATA TO THE BANK
5300
GET DATA FROM MERCHANT
5401
GET CREDIT CARD DATA
5404
GENERATE APPROVAL CODE
5406
VERIFICATION
NO
YES
5110
GENERATE MESSAGE, CANCEL PROCESSING, END
5203
ORDER CANCELLED
5303
GET DATA FROM CREDIT CARD ISSUER
5407
ORDER APPROVED
5111
GET DATA FOR APPROVAL
5112
VERIFIED?
NO
YES
5204
ORDER APPROVED
5408
ORDER NOT APPROVED
5513
ORDER APPROVED

Figure 3.

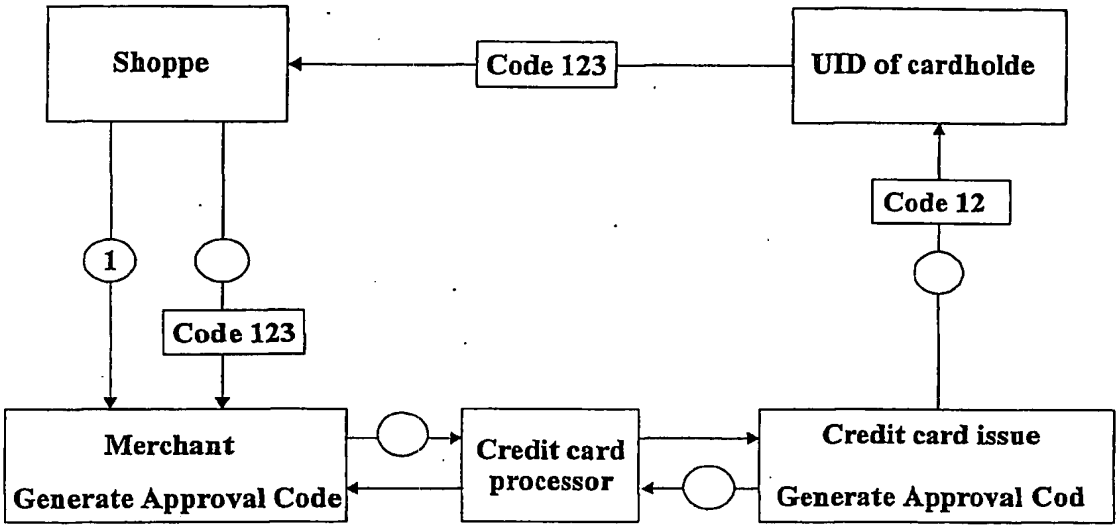


Figure 3.

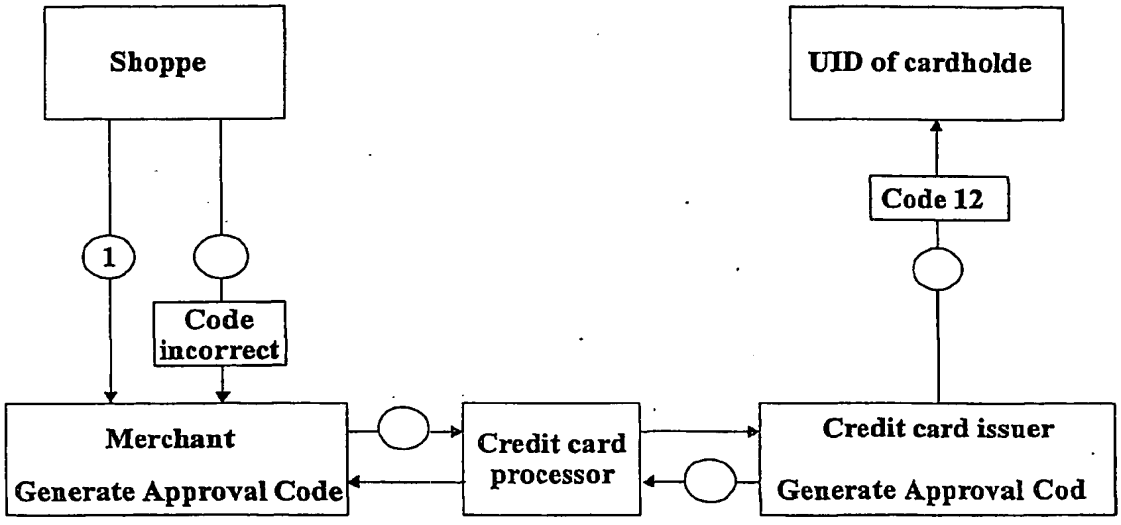
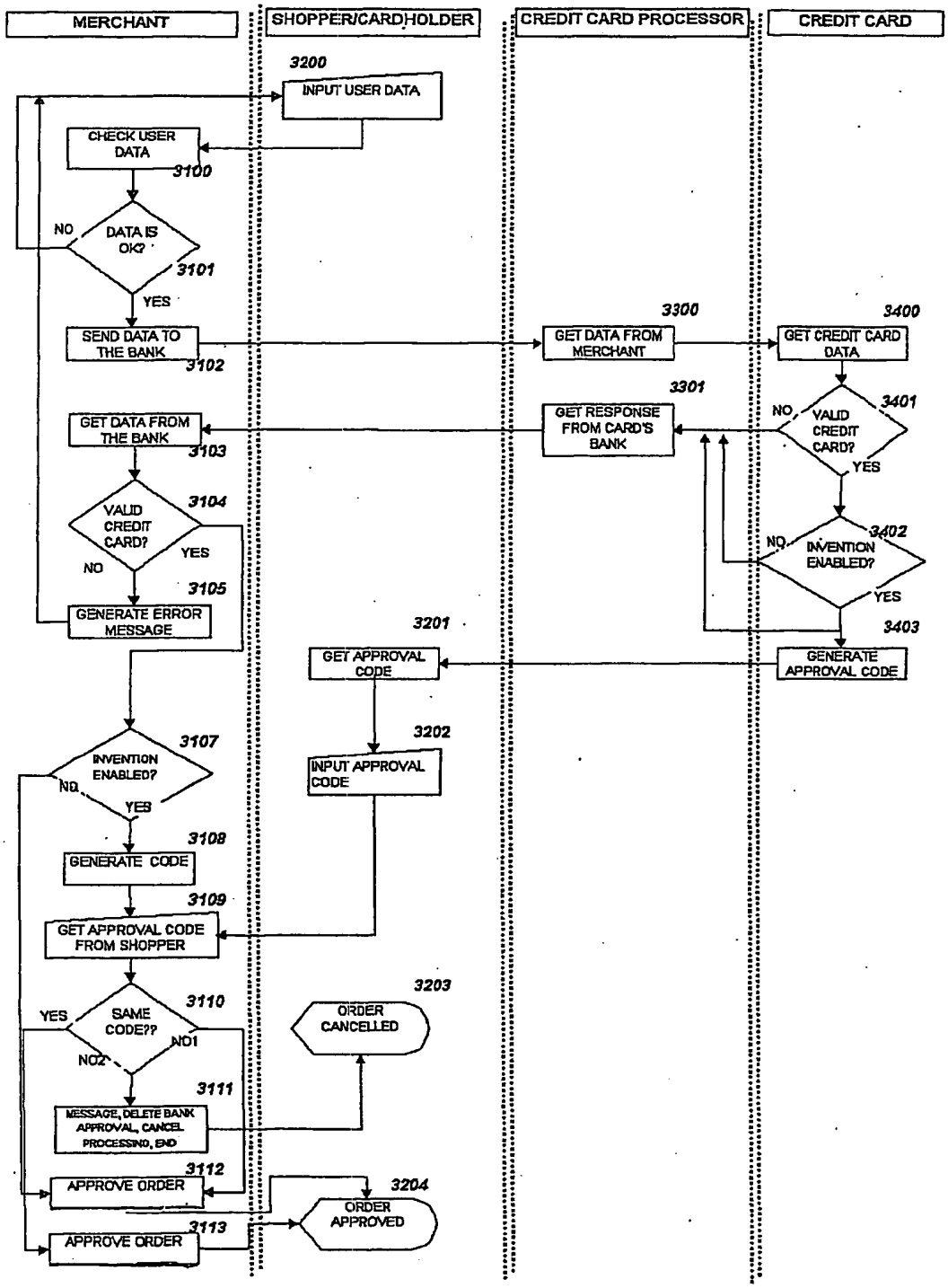
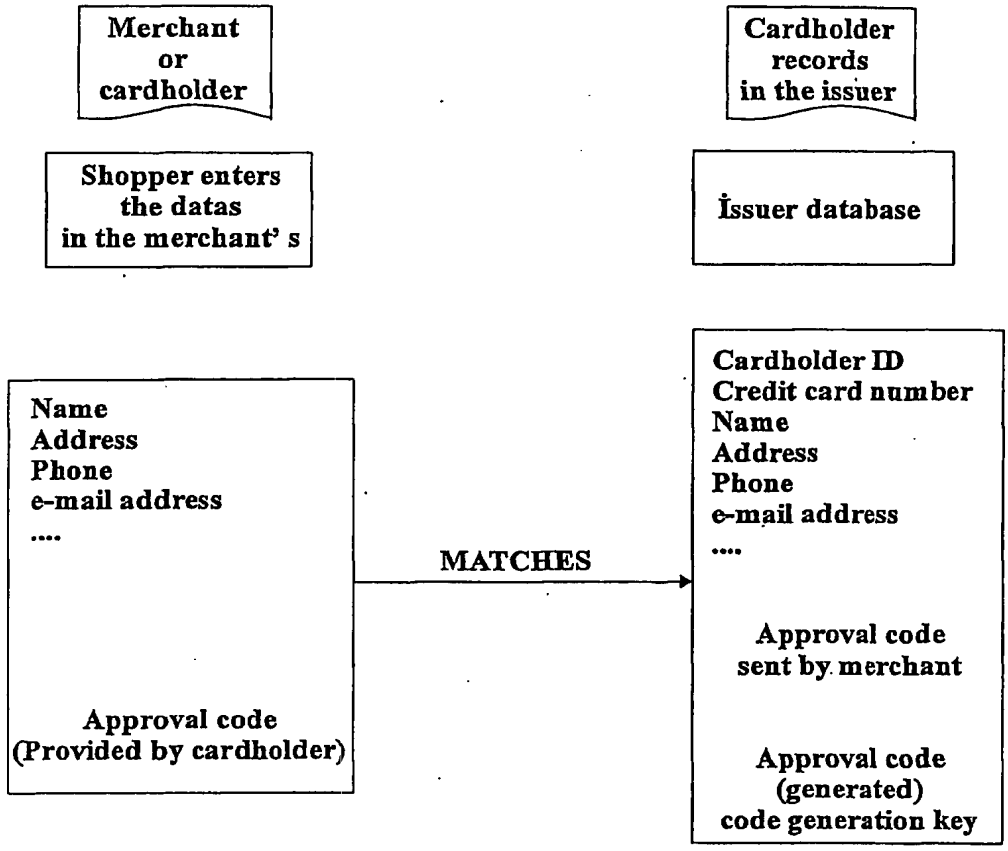


Figure 3.c


MERCHANT
SHOPPER/CARDHOLDER
CREDIT CARD PROCESSOR
CREDIT CARD
3200
INPUT USER DATA
CHECK USER DATA
3100
NO
DATA IS OK?
3101
YES
SEND DATA TO THE BANK
3102
3300
GET DATA FROM MERCHANT
3400
GET CREDIT CARD DATA
3301
GET RESPONSE FROM CARD'S BANK
NO
VALID CREDIT CARD?
3401
YES
GET DATA FROM THE BANK
3103
VALID CREDIT CARD?
3104
YES
NO
3105
GENERATE ERROR MESSAGE
NO
INVENTION ENABLED?
3402
YES
3403
GENERATE APPROVAL CODE
3201
GET APPROVAL CODE
3202
INPUT APPROVAL CODE
3107
INVENTION ENABLED?
NO
YES
3108
GENERATE CODE
3109
GET APPROVAL CODE FROM SHOPPER
3203
ORDER CANCELLED
YES
SAME CODE??
3110
NO1
NO2
3111
MESSAGE, DELETE BANK APPROVAL, CANCEL PROCESSING, END
3112
APPROVE ORDER
3204
ORDER APPROVED
3113
APPROVE ORDER

Figure



Figure

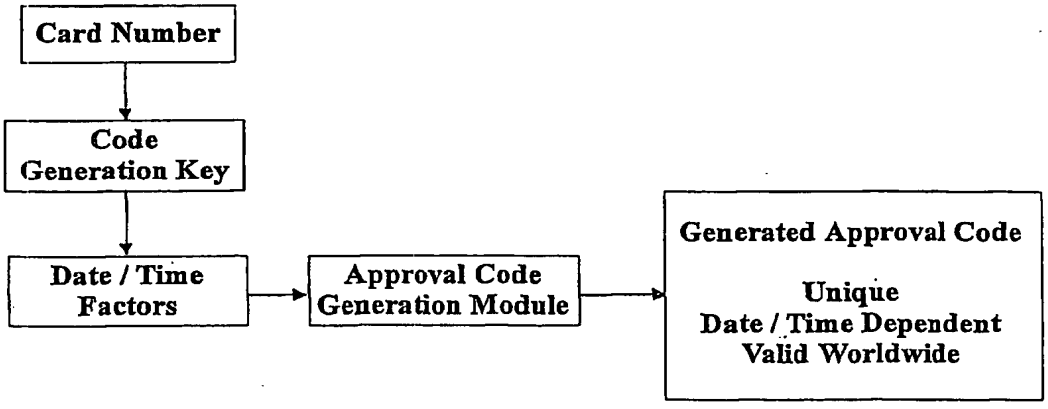
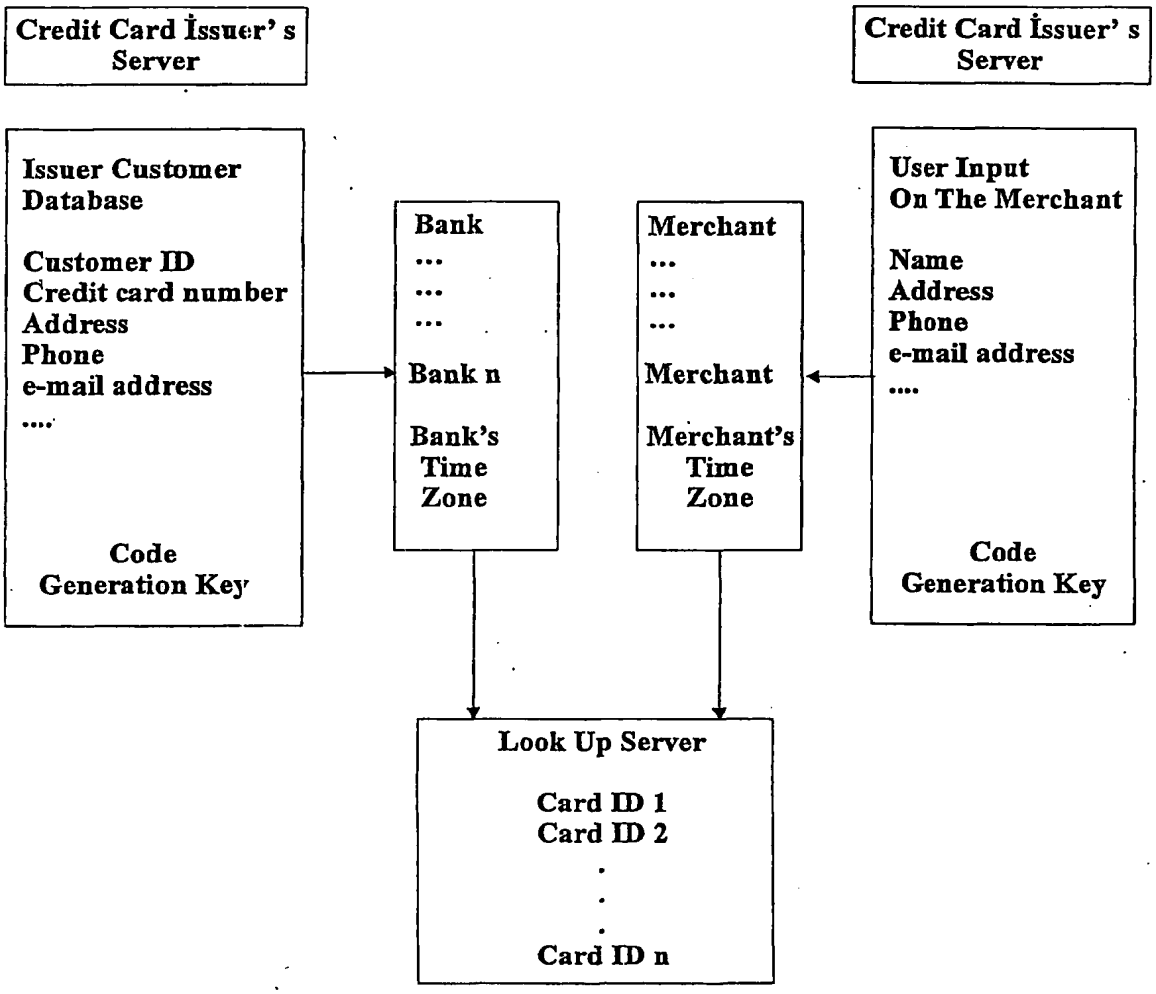


Figure 6


Credit Card İssuer' s Server
Credit Card İssuer' s Server
Issuer Customer Database
Customer ID
Credit card number
Address
Phone
e-mail address
....
Code Generation Key
Bank
...
...
...
Bank n
Bank's Time Zone
Merchant
...
...
...
Merchant
Merchant's Time Zone
User Input On The Merchant
Name
Address
Phone
e-mail address
....
Code Generation Key
Look Up Server
Card ID 1
Card ID 2
.
.
.
Card ID n

INTERNATIONAL S ARCH REPORT

Inte nal Application No
PC., .R 01/00003

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 745 961 A (AT & T CORP) 4 December 1996 (1996-12-04) column 3, line 22 - line 43 column 8, line 7 - line 28 column 10, line 13 - line 36 column 11, line 15 - line 22 column 17, line 7 - line 40	1,5-7, 11,22, 23,26
X	WO 95 16971 A (OPEN MARKET INC) 22 June 1995 (1995-06-22) page 9, line 31 -page 10, line 4 page 11, line 3 - line 30 page 12, line 19 - line 24 page 15, line 12 - line 15 page 15, line 29 - line 34 page 16, line 24 -page 17, line 2 page 20, line 3 -page 22, line 6	3,14-16, 19,20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 October 2001	19/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31 70) 340-3016	Schofield, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/ 01/00003

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 197 18 103 A (SCHMITZ KIM) 4 June 1998 (1998-06-04) column 1, line 39 -column 2, line 19 column 2, line 64 -column 3, line 10 column 4, line 53 - line 57	1,2, 4-13,22, 23
A	EP 0 690 399 A (TANDEM COMPUTERS INC) 3 January 1996 (1996-01-03) column 4, line 18 - line 45	1-27

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

mation on patent family members

Inter[illegible]al Appl[illegible]cation No
PC[illegible] 01 00003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0745961 A	04-12-1996	US 5708422 A	13-01-1998
		CA 2176163 A1	01-12-1996
		EP 0745961 A2	04-12-1996
		JP 8339407 A	24-12-1996
WO 9516971 A	22-06-1995	EP 0734556 A1	02-10-1996
		JP 11096243 A	09-04-1999
		JP 3190881 B2	23-07-2001
		JP 10312433 A	24-11-1998
		JP 3190882 B2	23-07-2001
		JP 10312434 A	24-11-1998
		JP 9500470 T	14-01-1997
		US 6205437 B1	20-03-2001
		US 6195649 B1	27-02-2001
		US 6199051 B1	06-03-2001
		US 6049785 A	11-04-2000
		WO 9516971 A1	22-06-1995
		US 5724424 A	03-03-1998
DE 19718103 A	04-06-1998	DE 19718103 A1	04-06-1998
		AU 6354598 A	05-11-1998
		BR 9801177 A	20-03-2001
		CN 1207533 A	10-02-1999
		EP 0875871 A2	04-11-1998
		JP 10341224 A	22-12-1998
		TW 425804 B	11-03-2001
		US 6078908 A	20-06-2000
EP 0690399 A	03-01-1996	CA 2153006 A1	31-12-1995
		CN 1118482 A	13-03-1996
		EP 0690399 A2	03-01-1996
		JP 8063532 A	08-03-1996
		US 5999624 A	07-12-1999